



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|------------------------------------------------------------------------------------------------------------------|-------------|----------------------|---------------------|------------------|
| 10/821,774 | 04/08/2004 | Calum Murray | 37202/136001:40098 | 1447 |
| 57956 7590 05/29/2008 OSHA - LIANG L.L.P. (INTUIT) 1221 MCKINNEY STREET SUITE 2800 HOUSTON, TX 77010 | | | | |
| EXAMINER LOUTE, OSCAR A | | | | |
| ART UNIT | | PAPER NUMBER | | |
| 2136 | | | | |
| NOTIFICATION DATE | | DELIVERY MODE | | |
| 05/29/2008 | | ELECTRONIC | | |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
lord@oshaliang.com
hathaway@oshaliang.com

Office Action Summary

Application No.

10/821,774

Applicant(s)

MURRAY ET AL.

Examiner

OSCAR A. LOUIE

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 February 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 3, 4, 7-10, 13, 15, 16, 19, 21, 22, 25, 27, 28, 31, 33, 34, 36, 37 and 39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3, 4, 7-10, 13, 15, 16, 19, 21, 22, 25, 27, 28, 31, 33, 34, 36, 37 and 39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

This first non-final action is in response to the Request for Continued Examination filing of 02/22/2008. The examiner notes that although the rejections have been maintained, the examiner has included additional explanations to help clarify motivation and reasons for the considerations below. Claims 1, 3, 4, 7-10, 13, 15, 16, 19, 21, 22, 25, 27, 28, 31, 33, 34, 36, 37 and 39 are pending and have been considered as follows.

Claim Objections

I. Claims 1, 7, 13, 19, 25, 31, 34, & 37 are objected to because of the following informalities:

- Claims 1, 7, & 31 line 2 recite “for” which should be “...configured to...”;
- Claims 13 & 34 line 1 recite “for” which should be “...configured to...”;
- Claims 19, 25, 37 line 1 recite “for” which should be “...of...”;

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1, 7, 19, 25, 31, 34, & 37 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- The above claims all recite, “accessing the database, based on the access rights associated with the temporary user name, to obtain the file,” however, according to the applicant’s specification, it does not appear as though the “temporary user name” is used to obtain “the file” as in a “file dump” which is an “encrypted database password.” It appears that the “temporary user name” is used to recover data specific to the particular user that the recovery agent has been authorized to acquire from the database.
- For the considerations below, the examiner interprets, “accessing the database, based on the access rights associated with the temporary user name, to obtain the file,” as using the “temporary user name” “associated with access rights” of a specific user, to access/recover information resources (i.e. data).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 7, 13, 19, 25, 31, 34, & 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A).

Claim 1:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor comprising,

- "receiving a request from a user to obtain a file from a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "wherein the user is associated with a user name" (i.e. "/* * Ensure we are running as Administrator before * we will run. */") [page 16];
- "obtaining, in response to the request, a file dump associated with the database" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];
- "wherein the file dump comprises an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];

Art Unit: 2136

- “decrypting the encrypted database password to obtain a database password” (i.e. “As this code decrypts the obfuscation step in the NT password database”) [page 2];
- “wherein the database password comprises a hash value derived from the user name and password” (i.e. “allowing a lanman and md4 hash to be written into the NT registry for a user account”) [page 2];
- “wherein the password is associated with the user” (i.e. “account password”) [page 2];

but Allison does not disclose,

- “obtaining a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “accessing the database using the temporary user name and the database password to obtain the file,” although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];

Art Unit: 2136

- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "accessing the database using the temporary user name and the database password to obtain the file," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 7:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor comprising,

- "initiating a signon attempt to a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "the signon attempt failing to connect" (i.e. "By default it will dump the password database of the local machine") [page 2];

- “wherein the failed signon attempt triggers an embedded mechanism within the database to dump an encrypted database password into a file” (i.e. “dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file”) [page 1];
- “reading the file to obtain the encrypted database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “decrypting the encrypted database password to obtain a database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “wherein the database password comprises a hash value derived from a user name and password” (i.e. “allowing a lanman and md4 hash to be written into the NT registry for a user account”) [page 2];
- “wherein the password is associated with the user name” (i.e. “account password”) [page 2];

but Allison does not disclose,

- “obtaining a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;

- “accessing the database using the temporary user name and the database password,” although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “obtaining a temporary user name based on the user name” and “wherein access rights associated with the user name are greater than access rights associated with the temporary user name” and “accessing the database using the temporary user name and the database password,” in the invention as disclosed by Allison for the purposes of having ““one-time” or “dynamic” passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval” [column 1 lines 41-45].

Claim 13:

Allison discloses a computer program product for controlling a processor to connect to a database comprising,

- “a computer readable medium” (i.e. “an NT machine that is held in the NT registry”) [page 1];
- “an attempted signon module stored on the computer readable medium” (i.e. “/* *Open a connection to the remote machines registry. */”) [pages 16-17];
- “the attempted signon module configured to communicate with the database to initiate a signon attempt to the database” (i.e. “/* *Open a connection to the remote machines registry. */”) [pages 16-17];
- “a read module stored on the computer readable medium configured to read a file dumped by the database” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “the file comprising an encrypted database password” (i.e. “security = user encrypted passwords = yes”) [page 2];
- “wherein the file is received in response to a failed sign on attempt” (i.e. “dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file”) [page 1];
- “a decryption module stored on the computer readable medium configured to decrypt the encrypted database password to obtain a database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];

Art Unit: 2136

- “wherein the database password comprises a hash value derived from a user name and password” (i.e. “allowing a lanman and md4 hash to be written into the NT registry for a user account”) [page 2];
- “wherein the password is associated with the user name” (i.e. “account password”) [page 2];

but Allison does not disclose,

- “a temporary signon module stored on the computer readable medium,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- “the temporary signon module configured to communicate with the database to initiate a user session with the database to obtain a temporary user name based on the user name,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “a pass connect string module stored on the computer readable medium,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- “the pass connect string module configured to communicate with the database to pass a connect string to a database tool,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

- “the connect string comprising the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- “wherein the database, upon receipt of the connect string, allows the database tool to query the database,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “a temporary signon module stored on the computer readable medium” and “the temporary signon module configured to communicate with the database to initiate a user session with the database to obtain a temporary user name based on the user name” and “wherein access rights associated with the user name are greater than access rights associated with the temporary user name” and “a pass connect string module stored on the computer readable medium” and “the pass connect string module configured to communicate with the database to pass a connect string to a database tool” and “the connect string comprising

the database password” and “wherein the database, upon receipt of the connect string, allows the database tool to query the database,” in the invention as disclosed by Allison for the purposes of having ““one-time” or “dynamic” passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval” [column 1 lines 41-45].

Claim 19:

Allison discloses a method for controlling a processor to connect to a database comprising,

- “executing a launcher program” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “reading, using the launcher program, a file dumped from the database” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “wherein the file comprises an encrypted database password” (i.e. “security = user encrypted passwords = yes”) [page 2];
- “decrypting the encrypted database password to obtain a database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “wherein the database password comprises a hash value derived from a user name and password” (i.e. “allowing a lanman and md4 hash to be written into the NT registry for a user account”) [page 2];
- “wherein the password is associated with the user name” (i.e. “account password”) [page 2];

but Allison does not disclose,

- “obtaining a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary, user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “accessing the database using the temporary user name and the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary, user name" and "accessing the database using the temporary user name and the database password," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 25:

Allison discloses a method for controlling a processor to connect to a database comprising,

- "initiating a signon attempt to a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "the signon attempt failing to connect" (i.e. "By default it will dump the password database of the local machine") [page 2];
- "reading the file to obtain the encrypted database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "decrypting the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "wherein the database password comprises a hash value derived from a user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];

- “wherein the password is associated with the user name” (i.e. “account password”) [page 2];

but Allison does not disclose,

- “obtaining a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “accessing the database using the temporary user name and the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "accessing the database using the temporary user name and the database password," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 31:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor comprising,

- "hashing a user name and password to create a database password" (i.e. "it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "encrypting the database password to create an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "storing the encrypted database password in a database" (i.e. "the password databases") [page 2];
- "receiving a signon attempt for the database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "wherein the signon attempt fails" (i.e. "By default it will dump the password database of the local machine") [page 2];

- “dumping a file comprising the encrypted password in response to the failed signon attempt” (i.e. “dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file”) [page 1];
- “decrypting the encrypted database password to obtain the database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];

but Allison does not disclose,

- “obtaining a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “accessing the database using the temporary user name and the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];

Art Unit: 2136

- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "accessing the database using the temporary user name and the database password," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 34:

Allison discloses a computer program product for controlling a processor to connect to a database comprising,

- "a computer readable medium" (i.e. "an NT machine that is held in the NT registry") [page 1];
- "a hash module stored on the computer readable medium configured to hash a user name and password to create a database password" (i.e. "it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "an encryption module stored on the computer readable medium configured to encrypt the database password to create an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];

- “a store module stored on the computer readable medium” (i.e. “an NT machine that is held in the NT registry”) [page 1];
- “the store module configured to communicate with a database to store the encrypted database password in the database” (i.e. “the password databases”) [page 2];
- “a send module stored on the computer readable medium” (i.e. “a 'AT' job on your NT server to periodically dump your NT password database into a new smbpasswd file and copy it over (securely somehow) to the Samba server”) [page 1];
- “the send module configured to communicate with a launcher application to send the encrypted database password file to the launcher application” (i.e. “copy it over (securely somehow) to the Samba server”) [page 1];
- “a launcher application stored on the computer readable medium” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];
- “configured to: decrypt the encrypted database password to obtain a database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 2];

but Allison does not disclose,

- “configured to: obtain a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;

- “configured to: access the database using the temporary user name and the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “configured to: obtain a temporary user name based on the user name” and “wherein access rights associated with the user name are greater than access rights associated with the temporary user name” and “configured to: access the database using the temporary user name and the database password,” in the invention as disclosed by Allison for the purposes of having ““one-time” or “dynamic” passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval” [column 1 lines 41-45].

Claim 37:

Allison discloses a method for controlling a processor to connect to a database and a launcher application comprising,

- “hashing a user name and password to create a database password” (i.e. “it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account”) [page 2];
- “encrypting the database password to create an encrypted database password” (i.e. “security = user encrypted passwords = yes”) [page 2];
- “storing the encrypted database password in a database” (i.e. “the password databases”) [page 2];
- “receiving a signon attempt for the database” (i.e. “/* *Open a connection to the remote machines registry. */”) [pages 16-17];
- “wherein the signon attempt fails” (i.e. “By default it will dump the password database of the local machine”) [page 2];
- “dumping a file comprising the encrypted password in response to the failed signon attempt” (i.e. “dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file”) [page 1];
- “decrypting, using the launcher application, the encrypted database password to obtain the database password” (i.e. “NTCrack. Or you can get l0phtcrack”) [page 1];

but Allison does not disclose,

- “obtaining, using the launcher application, a temporary user name based on the user name,” although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- “wherein access rights associated with the user name are greater than access rights associated with the temporary user name,” although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- “accessing the database using the temporary user name and the database password,” although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- “Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID” [column 1 lines 64-67 & column 2 lines 1-2];
- “IBM Resource Access Control Facility (RACF)” [column 6 line 52];
- “If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource” [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining, using the launcher application, a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "accessing the database using the temporary user name and the database password," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

6. Claims 3, 4, 15, 16, 21, 22, 27, 28, 33, 36, & 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A) and in further view of Kaufman et al. (US-5418854-A1).

Claims 3, 4, 9, 10, 15, 16, 27, & 28:

Allison and Guski et al. disclose a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor, a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor, a computer program product for controlling a processor to connect to a database, a method for controlling a processor to connect to a database, and a method for controlling a processor to connect to a database, as in Claims 1, 7, 13, 19, & 25, but their combination do not disclose,

- "wherein the database password is encrypted with a public key," although Kaufman et al. do suggest public key cryptography, as recited below;

- “wherein decrypting the encrypted database password is accomplished using a private key associated with the public key,” although Kaufman et al. do suggest private key encryption, as recited below;

however, Kaufman et al. do disclose,

- “A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys” [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, “wherein the database password is encrypted with a public key” and “wherein decrypting the encrypted database password is accomplished using a private key associated with the public key,” in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Claim 33:

Allison and Guski et al. disclose a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor, as in Claim 31, but their combination do not disclose,

- “wherein the encrypted password is encrypted with a public key,” although Kaufman et al. do suggest public key cryptography, as recited below;

however, Kaufman et al. do disclose,

- “A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys” [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, “wherein the encrypted password is encrypted with a public key,” in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Claims 36 & 39:

Allison and Guski et al. disclose a computer program product for controlling a processor to connect to a database and a method for controlling a processor to connect to a database and a launcher application, as in Claims 34 & 37, but their combination do not disclose,

- “wherein the database password is encrypted with a public key,” although Kaufman et al. do suggest public key cryptography, as recited below;
- “wherein the launcher application comprises a private key associated with the public key,” although Kaufman et al. do suggest private key encryption, as recited below;
- “wherein the launcher application decrypts the encrypted database password using the private key,” although Kaufman et al. do suggest public key cryptography and private key encryption, as recited below;

however, Kaufman et al. do disclose,

- “A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys” [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, “wherein the database password is encrypted with a public key” and “wherein the launcher application comprises a private key associated with the public key” and “wherein the launcher application decrypts the encrypted database password using the private key,” in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Response to Arguments

7. Applicant's arguments filed 02/22/2008 have been fully considered but they are not persuasive.

- The applicant's remarks regarding the prior art of record Allison has been considered but it appears that there is confusion over the portions of Allison that disclose the limitations of the applicant's application. It is noted, by the examiner, that the sections/portions recited in the “(i.e. “...”)” are meant to show the recitation of the reference(s) that at the very least provide suggestion for those limitations and are provided for the convenience of the applicant/applicant's representative and the entirety of the reference(s) is/are to be considered by the applicant/applicant's representative.

- The applicant's argument, "Guski does not teach "obtaining a temporary user name based on the user name" because the one-time password taught by Guski is neither based on the user name nor associated with the user," has been considered but is non-persuasive.
 - o The examiner notes that Guski states, "one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2] which provides suggestion that the one-time/temporary password is associated and based on (i.e. as a function of) various information including a user ID (i.e. a user or user name).
- The applicant's argument, "Guski does not teach "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" because the Examiner's citation, "IBM Resource Access Control Facility (RACF)," is insufficient to make a prima facie showing of obviousness," has been considered but is non-persuasive.
 - o The examiner notes that the intention of reciting the short portion as disclosed above in the applicant's argument, was to show that Guski provides suggestion for there being varying levels of access due to the incorporation of an access control system. At the very least, Guski provides suggestion for the one-time password as having less access rights than a non-one-time password since it is the nature of such passwords in a system with access control.

- The applicant's argument, "Guski does not teach "a temporary user name based on the user name," so consequently that reference also cannot teach a "temporary signon module...configured to...initiate a user session with the database to obtain a temporary user name based on the user name"," has been considered but is non-persuasive.
 - o The examiner notes that Guski discloses a one-time password that is a function of secret information or non-secret information including user passwords, user ID, etc and not just time dependent information.
- The applicant's argument, ",", has been considered but is non-persuasive.
 - o The examiner notes that Guski discloses authentication with one-time passwords which reads on the broad claim language of "a pass connect string." The examiner notes that "a pass connect string" appears to be a password connection string which basically is transmitting the password as a string for authentication purposes.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.
- a. Kwan (US-20030035548-A1) - client controlled data recovery
 - b. Chapman et al. (US-5774650-A) – temporary passwords, authentication, etc

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
05/21/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136